

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR  
A CRIMINAL COMPLAINT AND ARREST WARRANT**

I, Mark Comorosky, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a criminal complaint and arrest warrant charging LUIS ANGEL NARANJO RODRIGUEZ (DOB xx/xx/1990) with knowing possession of fifteen or more counterfeit or unauthorized access devices and with knowing possession of device-making equipment in violation of 18 U.S.C. §§ 1029(a)(3), 1029(a)(4), and 2 (the “Target Offenses”).

2. I am a Special Agent with the United States Secret Service (“USSS”), and have been since July 2006. I received formal training at the Federal Law Enforcement Training Center in Glynco, Georgia, and the USSS Academy in Beltsville, Maryland. Training included, among other things, the investigation of financial crimes which included the following; identity theft, access device fraud, bank fraud, forgery and counterfeit U.S. currency. I am currently assigned to the Boston Field Office. My current assignment includes investigating violations of Title 18, United States Code, Sections 1028, 1028A, 1029, 1037, 1341, 1343, 1344, 1349 and 1956. Based on my training and experience, I am familiar with the means by which individuals, including those engaging in financial and computer crimes, use computers and information networks to commit various crimes.

3. I am familiar with the facts and circumstances of this investigation through my personal participation, from discussions with other federal and state law enforcement officers, security personnel from Eastern Bank and American Express, and from my review of records and reports relating to the investigation. This is an ongoing investigation. Since this affidavit is being submitted for the limited purpose of seeking authorization for a criminal complaint and

arrest warrant, I have set forth the facts that I believe are necessary to establish probable cause and have not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that LUIS ANGEL NARANJO RODRIGUEZ has committed various crimes, including but not limited to the Target Offenses.

### **SUMMARY OF THE INVESTIGATION**

#### **General Background Regarding Nature of Scheme**

5. The USSS is currently investigating an ongoing conspiracy and scheme involving the fraudulent acquisition and use of thousands of credit or debit card account numbers from gas pumps located in Massachusetts, Connecticut, New Hampshire and Maine.<sup>1</sup> The technique to obtain these card numbers in these conspiracies is often referred to as “skimming.” I know from my training and experience and other USSS investigations that skimming involves the utilization of a hidden device to obtain account information encoded on a debit card or credit card that is swiped at a gas pump, automated teller machine (“ATM”), or other device used for processing transactions. These skimming schemes are often multi-layer conspiracies wherein skimmer installers and their associates steal confidential financial information, including business and personal account numbers and personal identification numbers (“PINs”), and transmit this information to co-conspirators through an array of online communication mechanisms, such as e-mail, instant messaging, and chat applications. Ultimately the stolen financial information is

---

<sup>1</sup> In addition to this scheme involving the fraudulent acquisition of account numbers from gas stations located in various states, the scheme involves the theft and fraudulent use of account numbers issued by banks that I know to do business in multiple states and to be insured by the Federal Deposit Insurance Corporation. Moreover, as described below, this scheme involves the transmission of stolen credit/debit account numbers via text message (SMS); such messages are transmitted via mobile phone providers that operate in interstate commerce.

often used to encode plastic cards with magnetic stripes, such as gift cards, counterfeit credit or debit cards, and hotel key cards, which can be used to withdraw currency from ATMs or to make purchases.

6. The particular skimming scheme at issue in this case appears to have utilized two different types of skimming devices to obtain and transmit information concerning consumer credit or debit cards from gas pumps on which these devices were hidden.<sup>2</sup>

7. The first type of skimming device will be referred to as a “Bluetooth Skimmer.” The “Bluetooth Skimmer” captures data from a victim’s card and stores the data on an internal memory card. The stolen data can then be extracted from the Bluetooth Skimmer by connecting to it within wireless Bluetooth range or by removing the device itself to access the memory card.

8. The second type of skimming device will be referred to as an “SMS Skimmer.”<sup>3</sup> An SMS Skimmer generally uses a SIM card to transmit data derived from a victim’s card. Specifically, when a victim swipes his or her card, the SMS skimmer sends a text message with such data via the installed SIM card to a phone number where it was programmed. As such, a perpetrator utilizing an SMS Skimmer can obtain the data derived from victims’ cards without returning to the location of the SMS skimmer.

### **PROBABLE CAUSE**

#### **Background re: Skimming Devices at Concord Gulf**

---

<sup>2</sup> It is my understanding that skimming devices designed to obtain and/or transmit account information without authority constitute “device making equipment” pursuant to 18 U.S.C. § 1029(e)(6). It is further my understanding that credit or debit card account numbers that are obtained via a hidden and unauthorized skimming device constitute counterfeit or unauthorized access devices pursuant to 18 U.S.C. § 1029(e)(1) – (3).

<sup>3</sup> SMS refers to Short Message Service, commonly referred to as text messages.

9. On April 19, 2019, a gas pump technician discovered Bluetooth Skimmers on two gas pumps at the Gulf gas station located on the Concord Rotary at 503 Commonwealth Avenue, Concord, MA (the “Concord Gulf”). USSS later examined these two Bluetooth Skimmers and found them to contain 391 account numbers. A review of surveillance footage from the Concord Gulf showed a 2019 Nissan Armada color black with Massachusetts registration 7KZ572 accessing the two pumps on April 6, 2019 at approximately 10:45 pm.

10. Investigation revealed that this Nissan Armada was rented out of Logan Airport in Boston, MA from Alamo Rental on April 5, 2019 by PERSON 1 at approximately 10:19 am.

11. PERSON 1 was arrested on April 16, 2019 in Broward County, Florida on charges related to skimming fraud. A Broward County Sheriff detective involved with the investigation of PERSON 1 informed Concord Police that PERSON 1 was working with two other individuals, one of whom was identified as LUIS ANGEL NARANJO RODRIGUEZ, in a gas pump skimming operation.

12. Surveillance footage from Alamo Rental at Logan Airport showed two males at the rental counter on April 5, 2019 at approximately 10:19. I have compared this surveillance footage with Florida driver’s license photos for PERSON 1 and NARANJO RODRIGUEZ, and I believe the two males depicted in the surveillance footage to be PERSON 1 and NARANJO RODRIGUEZ.

13. On May 19, 2019, employees at the Gulf gas station located at 1287 Worcester Road, Framingham, MA (the “Framingham Gulf”) discovered two Bluetooth Skimmers. USSS later examined these two Bluetooth Skimmers and found the internal memory card to contain 10 account numbers. Of those 10, 6 of the account numbers were the same – xxxx xxxx xxxx 9854.

The name associated with that account was RODRIGUEZ/L NARANJO.<sup>4</sup> The Bancorp Bank is the issuing bank for that card.

**November 17, 2019 Arrest of NARANJO RODRIGUEZ**

14. On November 17, 2019, at approximately 01:05am, a Concord Police officer (the “CPD Officer”) observed a vehicle parked at the gas pumps located at the Concord Gulf. The CPD Officer understood that the Concord Gulf closed at 11:00pm. The CPD Officer pulled into the Concord Gulf lot and observed a male (“PERSON 2”) sitting in the driver’s seat of a Black Ford Explorer and another male – later identified as NARANJO RODRIGUEZ – standing by a pump. The CPD Officer observed NARANJO RODRIGUEZ wearing black latex gloves. NARANJO RODRIGUEZ indicated to the CPD Officer that he (NARANJO RODRIGUEZ) was getting gas.

15. Other officers arrived at the Concord Gulf, and the CPD Officer observed a set of keys on the lock of the gas pump by which NARANJO RODRIGUEZ had been standing.<sup>5</sup> Subsequently, officers<sup>6</sup> placed NARANJO RODRIGUEZ under arrest. Officers seized a red

---

<sup>4</sup> Based on my training and experience, I understand that part of the process of installing a gas pump skimmer is to ensure that the device is functioning properly. This is often done by testing it with a valid credit card that the installer has on his person.

<sup>5</sup> I understand, based on my training, experience, and knowledge of gas pump skimming operations, that perpetrators of such schemes often open a gas pump to install a skimming device, remove a skimming device, and/or retrieve stolen data from a skimming device, and that such perpetrators often obtain a universal or master key that will enable them to access pumps at a range of gas stations, either by ordering such key online or otherwise. I also know, based on my everyday experience, that customers obtaining gas for their vehicles do not need or use such pump keys. Based on the pertinent facts, and my training and experience, I believe that NARANJO RODRIGUEZ was using the key depicted below to open the gas pump in order to install a skimming device to be used for the acquisition and fraudulent use of account data.

<sup>6</sup> The word “officers” in this affidavit refers to actions undertaken by one or more police officers.

iPhone with a Dewalt tool sticker on the back of the iPhone from the person of NARANJO RODRIGUEZ (the "NARANJO RODRIGUEZ iPHONE").

16. Also on November 17, 2019, officers conducted a search of the Ford Explorer. Officers located what appeared to be a credit card skimming device under the driver's seat, and placed PERSON 2 under arrest. Officers searching the Ford Explorer also located four SMS skimming devices in the glovebox, black rubber gloves in a seat of the vehicle, additional gas pump keys, a black Samsung phone, and a red iPhone. Also found in the vehicle, specifically in the sunglass holder compartment attached to the rear view mirror, were seven bank cards.

17. Also on November 17, 2019, PERSON 2 indicated to police that he and NARANJO RODRIGUEZ had traveled from Miami on Thursday November 14, 2019 and that PERSON 2 was working for NARANJO RODRIGUEZ, who was paying him and all his expenses. PERSON 2 also provided information about where he and NARANJO RODRIGUEZ had been staying.

18. Police contacted the clerk at a hotel in Framingham, Massachusetts (the "Hotel") and learned that "Luis Rodriguez" had been staying in Room 328. The clerk also informed the officer that someone claiming to be the guest's brother had just called the Hotel claiming that Luis was in an accident and the room would need to be extended until someone could come up from Miami to clean out the room.

19. Officers later obtained a search warrant for Room 328 at the Hotel. Among the items seized from the room were a Dell laptop and \$1,470 in US currency.

20. An employee of the Hotel indicated that hotel records indicated that NARANJO RODRIGUEZ had stayed at the Hotel six times since July 9, 2019, and that he (the employee) believed that NARANJO RODRIGUEZ had also stayed at the Hotel with PERSON 1.

The Hotel employee also indicated that, following check-out on September 30, 2019, a housekeeper cleaning out a room discovered a sock containing eleven different credit cards – nine in the name of “Luis A NARANJO” and two in the name of PERSON 1.

**Examination of Cards and Devices Seized on November 17, 2019**

21. I have run the seven bank cards found during the search of Ford Explorer through a card reader. The seven cards were gift cards and did not have any names on them. Those seven cards had account numbers encoded on the magnetic stripe, which did not match the issuing bank.<sup>7</sup> For example, one card was labeled “Green Dot” on the front of the card, but was encoded with a Santander Bank account number. The stripe data revealed account numbers from Santander Bank, Eastern Bank, and Citizen’s Bank. Based on my training and experience, and the facts developed during this investigation, I believe that each of these gift cards had been encoded with the account data of a legitimate credit/debit account so that the user of the gift card could fraudulently use the funds or credit associated with such legitimate account (for example, to withdraw money from a debit account or to make a purchase on a credit or debit account). This is commonly how participants in a fraudulent skimming scheme profit from the account data that has been stolen via skimming devices.

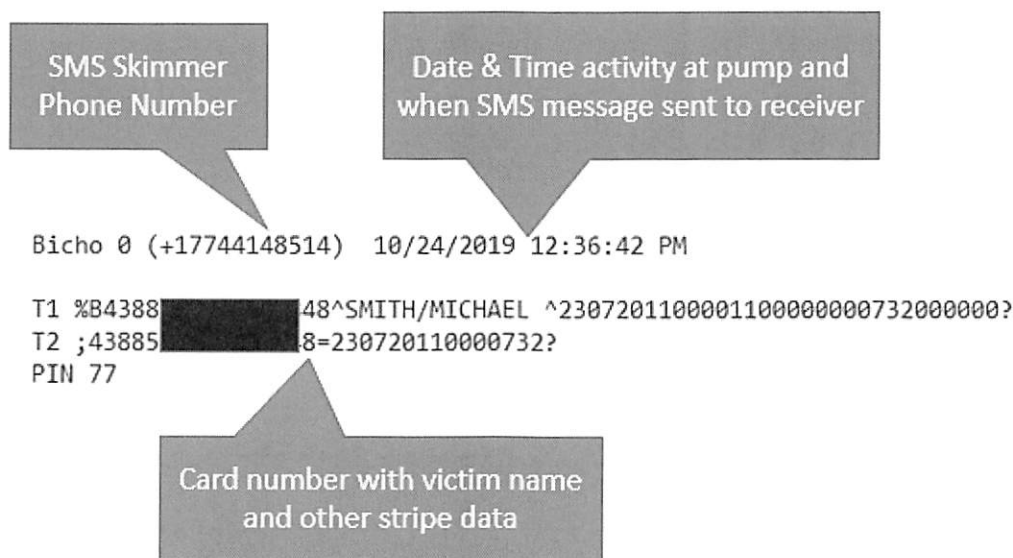
22. Investigation later revealed that, of the seven gift cards, five appear to have been used by NARANJO RODRIGUEZ at ATMs located at two retail stores in Framingham, MA on November 16, 2019. Specifically, surveillance footage obtained from the two stores shows an individual whose appearance and clothing are consistent with that of NARANJO RODRIGUEZ

---

<sup>7</sup> Each bank that issues credit and debit cards use a bank identification number (“BIN”) that uniquely identifies the institution issuing the card. The BIN is the first six numbers of the card number. On each of the cards referenced above, I searched the BIN in a database to find the issuing bank. All seven BINs found on the card’s stripe data did not match the issuing bank shown on the physical card.

when he was arrested hours later utilizing an ATM at approximately the same time that, according to bank records, transactions from pertinent accounts were made and/or attempted at such locations.<sup>8</sup> I believe that the individual depicted in the pertinent surveillance footage is NARANJO RODRIGUEZ based, in part, on his face being visible at one location.

23. USSS examined the Dell laptop seized in search of the Hotel room pursuant to a Massachusetts search warrant. The exam resulted in the discovery of 386 account numbers in a text file titled "Samsung SM-N950U\_SMS\_20191027102659." The file indicated date and times of SMS activity and the name of the victim in addition the account number. It appears, based on my review of this file, and my training and experience, that this file reflects credit/debit card account information that was stolen via a SMS Skimmer and then transmitted via SMS. The following image depicts a sample entry from the text file (with my annotations in the shaded



boxes).

<sup>8</sup> Based on my investigation, it appears that the individual who appears to be NARANJO RODRIGUEZ made or attempted transactions at these two retail stores using account information that was stolen via a skimming device that had been installed at a Sunoco gas station in Randolph, Massachusetts. Specifically, Santander Bank records reflect attempted transactions of \$966.50, with \$523.25 being approved. Eastern Bank records reflect \$206.25 in approved transactions. Citizens Bank records reflect an attempted transaction of \$200.



24. NARANJO RODRIGUEZ's name appears numerous times in files on the Dell laptop. For example, the only user account file for the laptop is "luis a NARANJO." Also listed in the account file is the phone number 786-333-5812. That phone number is the phone number for the NARANJO RODRIGUEZ iPHONE (*i.e.*, the iPhone that was seized from NARANJO RODRIGUEZ's person on November 17, 2019).

25. USSS also examined the black Samsung phone, seized from the Ford Explorer, pursuant to a Massachusetts search warrant. The exam resulted in the discovery of 4,878 account numbers reflected in what appear to be incoming messages. It appears, based on my review of the phone, and my training and experience, that various messages on the phone reflect account information that was stolen via a SMS Skimmer and then transmitted via SMS. The 386 account numbers found on the Dell laptop were also found on the Samsung phone.

26. Stored in the internal memory of the Samsung phone was a call log to 786-333-5812, the number associated with the NARANJO RODRIGUEZ iPHONE. Also discovered was a stored GPS location near the Hotel on November 2, 2019. A review of data of the NARANJO RODRIGUEZ iPHONE also showed cell tower connections in the area of the Hotel on November 2, 2019.

27. Working with bank investigators from Santander Bank, Eastern Bank, American Express, and Synergent Corporation, USSS has become aware of the locations for nineteen SMS skimmers that appear to have been utilized in this skimming scheme. This was accomplished by obtaining transaction history – including information about the location of relevant transactions – for certain account numbers that were listed in a text message received on the Samsung phone. It appears that credit/debit card data was stolen via skimmers involved at gas stations in the following locations and transmitted to the Samsung phone: Willington, CT, Lynnfield, MA,

Concord, MA, Malden, MA, Taunton, MA, Randolph, MA, Raynham, MA, Portland, ME, Nashua, NH, and Willington, CT. Skimming equipment was recovered from some, but not all, of these gas stations.

28. USSS examined the red iPhone, seized from the Ford Explorer, pursuant to a Massachusetts search warrant. It appears that this iPhone was used by PERSON 2. Location data found on this iPhone shows that the phone was located at or near various locations relevant to this investigation, including (1) the Hotel; (2) the gas station in Taunton, MA at which a SMS skimmer was known to be operating based on recovered SMS texts; and (3) the two retail locations in Framingham, MA at which NARANJO RODRIGUEZ appears to have conducted ATM transactions on November 16, 2019.

29. USSS examined the NARANJO RODRIGUEZ iPhone pursuant to a Massachusetts search warrant. Cell phone tower data obtained for this phone shows extensive use at or near the home address of NARANJO RODRIGUEZ in Hialeah, Florida (*i.e.*, the address listed on the Florida driver's license for NARANJO RODRIGUEZ). In addition, this phone has wifi connection history showing connections including to the Hotel on November 16, 2019 and to a wifi signal listed as "lauraXXXXXXXX" on a number of dates in October and November 2019.<sup>9</sup> I understand that the name of this wifi signal corresponds to the name of a female ("PERSON 3") who is known to be in a relationship with NARANJO RODRIGUEZ.<sup>10</sup>

---

<sup>9</sup> The wifi signal name above has been redacted for privacy purposes.

<sup>10</sup> Specifically, the name of the wifi signal corresponds to the first name and initial surname of PERSON 3. According to a CPD report, citing information derived from staff at the Hotel, PERSON 3 checked into the Hotel on November 21, 2019 and requested access to Room 328, presenting a copy of NARANJO RODRIGUEZ's birth certificate.

30. Further analysis of the cell phone tower records for the NARANJO RODRIGUEZ iPhone show it to have been located or near at multiple locations pertinent to this investigation. For example, the records indicate that this phone connected to cell towers near the Hotel on various dates from July 9 to July 13, 2019, from September 20 through September 28, 2019, from October 21 through October 24, 2019, from October 31 through November 4, 2019, and from November 14 through November 16, 2019. Tower records also show that the phone was at or near a Gulf gas station in Raynham, MA on September 18, September 19, and September 20, 2019; an SMS skimmer was discovered at this Gulf station on or about October 10, 2019. An exam of the SMS skimmer revealed the phone number assigned to that skimmer, which appears on text messages found in the Samsung phone (thus indicating that the skimming device recovered from Raynham had been sending messages to the Samsung phone). Similarly, tower records show that the NARANJO RODRIGUEZ iPhone was at or near a Mobil gas station in Malden, MA on October 23, 2019. Based on an analysis of the SMS messages found on the Samsung phone and a comparison to records from Eastern Bank and American Express, I believe that SMS skimmers were operating at the Mobil gas station in Malden, MA on October 24 and October 25, 2019.

### **CONCLUSION**

31. In summary, the evidence in this case demonstrates the involvement of NARANJO RODRIGUEZ in a scheme and conspiracy involving the installation of skimming equipment and the use of this equipment to obtain and use stolen credit/debit card account information. This scheme has involved the acquisition and compilation of at least 5,659 account numbers. Based on my knowledge of this scheme and my training and experience, I believe that these account numbers were likely obtained when victims swiped their credit/debit cards at gas


pumps at which NARANJO RODRIGUEZ or his associates had installed skimming devices. It appears likely that NARANJO RODRIGUEZ and his co-conspirators compromised account data belonging to thousands of victims.

32. Further, I believe that the evidence establishes probable cause to believe that, on November 17, 2019 in Concord, Massachusetts, Luis Angel NARANJO RODRIGUEZ, (A) knowingly and with intent to defraud, possessed fifteen or more counterfeit or unauthorized access devices – specifically, hundreds of credit or debit account numbers – in a manner that affects interstate commerce, in violation of 18 U.S.C. §§ 1029(a)(3) and 2, and (B) had control and custody over and possessed device-making equipment – specifically, one or more skimming devices – in a manner that affects interstate commerce, in violation of 18 U.S.C. §§ 1029(a)(4) and 2.

Respectfully submitted,

  
Mark Comorosky  
Special Agent  
U.S. Secret Service

Subscribed and sworn to before me on March 6<sup>th</sup>, 2020.

  
Honorable Jennifer C. Boal  
UNITED STATES MAGISTRATE JUDGE

